IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered)

Please AMEND claims 1, 24, 27 and 34 and ADD new claims 38-53 in accordance with the following:

1. (currently amended) A signature system presenting a receiver with signature information of a user, comprising:

an input unit inputting authentication information of the user; and

an output unit outputting information for generation of the signature information according to the input authentication information, the output information including a signature program, and

wherein the signature program generates first blind information from illegal use prevention information for protection against illegal use, and enters both the first blind information and the illegal use prevention information in the signature information, and

wherein the output information is prepared such that, after the signature information is generated according to the output information to present the signature information to the receiver, the signature program can be removed from memory.

Claims 2-5 (canceled)

6. (previously presented) The system according to claim 1,

wherein said signature program contains a one-directional function and an encryption key, used in generating blind information from said illegal use prevention information.

Claims 7-23 (canceled)

24. (currently amended) A computer-readable storage medium storing a program used to direct a computer to perform a method comprising:

inputting identification information of a user;

generating output information for generation of signature information of the user according to the input identification information;

generating a signature program for generating blind information from the illegal use prevention information, and entering both the blind information and the illegal use prevention information in the signature information; and

outputting the output information and the signature program in a format readable by a bar code reader, and

wherein the output information is prepared such that, after the signature information is generated according to the output information, the signature program can be removed from memory.

27. (currently amended) A signature system presenting a receiver with signature information of a user, comprising:

input means for inputting the identification information of the user; and

output means for outputting information for generation of the signature information according to the input identification information, including a signature program, in a format readable by a bar code reader, and

wherein the signature program generates blind information from illegal use prevention information, and enters both the generated blind information and the illegal use prevention information in the signature information, and

wherein the output information is prepared such that, after the signature information is generated according to the output information to present the signature information to the receiver, the signature program can be removed from memory.

Claims 28-33 (cancelled)

34. (currently amended) The system according to claim ~~1~~ 45,

wherein said comparison unit further generates blind information from said illegal use prevention information contained in the signature information, and compares the generated blind information with the blind information contained in the signature information.

35. (previously presented) A signature system, comprising:

management unit for managing first blind information generated from authentication information, one-directional function and encryption key which are registered by a user;

receiving unit for receiving signature information which contains the authentication information;

generation unit for generating second blind information from the authentication information contained in the signature information, using the one-directional function and the encryption key;

comparison unit for comparing the first blind information with the second blind information to produce a first comparison result; and

verification unit for verifying the signature information according to the first comparison result.

36. (previously presented) A signature system according to claim 35, wherein:

said receiving unit receives signature information which contains illegal use prevention information and third blind information generated from the illegal use prevention information;

said generation unit further generates fourth blind information generated from the illegal use prevention information contained in the signature information, using the one-directional function and the encryption key;

said comparison unit further compares the third blind information with the fourth blind information to produce a second comparison result; and

said verification unit verifies the signature information according to the second comparison result.

37. (previously presented) A signature system according to claim 35,

wherein said receiving unit receives from the user, authentication information and the first blind information generated from authentication information, and

wherein said generation unit generates third blind information from the authentication information, using the one-directional function and the encryption key, and

wherein said comparison unit compares the first blind information with the third blind information to produce a second comparison result, and

further comprising entering unit for entering the first blind information in said management unit, if the first and third blind information are identical according to the second comparison result.

38. (new) A signature system according to claim 37,

wherein said entering unit deletes the authentication information received by said receiving unit, after entering the blind information.

39. (new) A computer-readable storage medium storing a program used to direct a computer to perform a method comprising:

inputting authentication information by a user;

generating blind information from the authentication information, using a one-directional function and an encryption key; and

entering in a device the blind information from the authentication information, the one-directional function and the encryption key.

40. (new) A signature system, comprising:

input means through which a user inputs authentication information;

generating means for generating blind information from the authentication information, using a one-directional function and an encryption key; and

enter means for entering in a device the blind information from the authentication information, the one-directional function and the encryption key.

41. (new) The system according to claim 1, wherein said input unit inputs image data of an image of a seal as the authentication information.

42. (new) The signature system according to claim 1, wherein said output unit outputs the information for generation of the signature information in a format readable by a bar code reader.

43. (new) A signature system presenting signature information of a user to a receiver, comprising:

a reading unit reading information, including program information, for generation of the signature information, where the program information can be removed from memory after the signature information is generated according to the information for generation of the signature information; and

a generation unit generating blind information from illegal use prevention information for protection against illegal use, and generating the signature information which contains the blind information and the illegal use prevention information, according to the program information.

44. (new) The system according to claim 43, further comprising a timer unit generating date and time information used as the illegal use prevention information.

45. (new) The system according to claim 43,

wherein said reading unit further reads authentication information of the user,

wherein said generation unit further includes the authentication information of the user in the signature information, and

further comprising:

a management unit managing first blind information of the authentication information;

a comparison unit generating second blind information from the authentication information contained in the signature information, comparing the second blind information with the first blind information and obtaining a comparison result; and

a verification unit verifying the signature information based on the comparison result.

46. (new) The system according to claim 45,

further comprising an issue unit issuing certification information containing the first blind information of the authentication information,

wherein said reading unit reads the certification information,

wherein said generation unit further includes the certification information in the signature information, and

wherein said comparison unit compares the second blind information generated by said comparison unit with the first blind information contained in the certification information.

47. (new) The signature system according to claim 43, wherein said reading unit reads the program information in a bar code format.

48. (new) The signature system according to claim 43,

wherein said program information contains a one-directional function and an encryption key, and

wherein said generation unit generates the blind information from the illegal use prevention information using the one-directional function and the encryption key.

49. (new) A signature system, comprising:

a terminal of a user, including

an input unit through which the user inputs authentication information;

a generation unit generating blind information of the authentication information using a one-directional function and an encryption key; and

an entry unit entering in a device, the blind information, the one-directional function and the encryption key.

50. (new) A computer-readable storage medium storing a program used to direct a computer to perform a method comprising:

reading information in a bar code format, including program information, for generation of signature information, where the program information can be removed from memory after the signature information is generated according to the information for generation of the signature information; and

generating the signature information, by generating blind information from illegal use prevention information for protection against illegal use, and entering the blind information and the illegal use prevention information in the signature information, based on the program information.

51. (new) A computer-readable storage medium storing a program used to direct a computer to perform a method comprising:

managing first blind information generated from authentication information, a one-directional function and an encryption key which are registered by a user;

receiving signature information which contains the authentication information;

generating second blind information from the authentication information contained in the signature information, using the one-directional function and the encryption key;

comparing the first blind information with the second blind information to produce a comparison result; and

verifying the signature information according to the comparison result.

52. (new) A signature system presenting signature information of a user to a receiver, comprising:

reading means for reading information in a bar code format, including program information, for generation of the signature information, where the program information can be removed from memory after the signature information is generated according to the read information; and

generation means for generating illegal use prevention information for protection against illegal use according to the read information; for generating blind information from the illegal use prevention information using the program information, and for generating the signature information including both the blind information and the illegal use prevention information.

53. (new) A signature system, comprising:

management means for managing first blind information generated from authentication information, a one-directional function and an encryption key which are registered by a user;

receiving means for receiving signature information which contains the authentication information;

generation means for generating second blind information from the authentication information contained in the signature information, using the one-directional function and the encryption key;

comparison means for comparing the first blind information with the second blind information to produce a comparison result; and

verification means for verifying the signature information according to the comparison result.